ITRI 625

Pfleeger Chapter 10

Whitman & Mattord Chapters 4 & 5

Security planning

- A good security plan is an official record of current security practices, plus a blueprint for orderly change to improve those practices.

- Every security plan must address seven issues.

1. Policy.
2. Current state.
3. Requirements.
4. Recommended controls.
5. Accountability.
6. Timetable.
7. Continuing attention.

Security planning *cont.*

- A security planning team should represent each of the following groups:

1. Computer hardware group.
2. System administrators.
3. Systems programmers.
4. Applications programmers.
5. Data entry personnel.
6. Physical security personnel.
7. Representative users.

- Three groups of people must contribute to make the plan a success.

1. The planning team being sensitive to the needs of each group.
2. Those affected must understand the plan's implications.
3. Management being committed to using and enforcing the plan.

Risk analysis

- A risk is a potential problem that the system or its users may experience.

- We distinguish a risk from other project events by looking for three things:

1. A loss associated with an event.
2. The likelihood that the event will occur.
3. The degree to which we can change the outcome.

- The three strategies for dealing with risk are:

1. Avoiding the risk.
2. Transferring the risk.
3. Assuming the risk.

Risk analysis *cont.*

- Risk analysis is the process of examining a system and its operational context to determine possible exposures and the potential harm they can cause.

- The basic steps of a risk analysis are:

1. Identify assets.
2. Determine vulnerabilities.
3. Estimate likelihood of exploitation.
4. Compute expected annual loss.
5. Survey applicable controls and their costs.
6. Project annual savings of control.

Risk analysis *cont.*

- There are many good reasons to perform a risk analysis in preparation for creating a security plan.

1. Improve awareness.
2. Relate security mission to management objectives.
3. Identify assets, vulnerabilities and controls.
4. Improve basis for decisions.
5. Justify expenditures for security.

- However, despite the advantages there are also several arguments against it.

1. False sense of precision and confidence.
2. Hard to perform.
3. Immutability.
4. Lack of accuracy.

Organizational security policies

- A security policy is a high-level management document to inform all users of the goals of and constraints on using a system.

- They are used for several purposes, including:

1. Recognizing sensitive information assets.
2. Clarifying security responsibilities.
3. Promoting awareness for existing employees.
4. Guiding new employees.

- A security policy addresses several different audiences with different expectations. Each group uses the security policy in important but different ways.

Organizational security policies *cont.*

- A security policy must identify its audiences and describe the nature of each audience and their security goals.
- The policy should state the purpose of the organization's security functions, reflecting the requirements of beneficiaries, users and owners.
- A security policy must be comprehensive, and if it is written poorly, it cannot guide the developers and users in providing appropriate security mechanisms to protect important assets.
- A security policy must grow and adapt well, as an obscure or incomplete policy will not be implemented properly, if at all.

Physical security

- As discussed in ITRI615, physical security is the term used to describe protection needed outside the computer system.

- Many physical security measures can be provided simply by good common sense.

- With regards to physical security from an administration perspective, the following need to be considered:
  - Natural disasters.
  - Power loss.
  - Surge suppressor.
  - Human vandals.
  - Interception of sensitive information.
  - Contingency planning. The key to successful recovery is adequate planning.

Questions

- Any Questions?